Technische Universität München
Fakultät für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr
Dr. Werner Meixner

Wintersemester 2012/13
Übungsblatt 7
26. November 2012

Diskrete Strukturen

Abgabetermin: 4. Dezember 2012, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (5 Punkte)

1. Definieren Sie eine Algebra $A = (S, \circ)$ mit $|S| = 4$, so dass jedes Element $x \in S$ ein rechtes Einselement ist, d.h., dass für alle $x, y \in S$ die Gleichung $y \circ x = y$ gilt.

   Ist Ihre Algebra eine Halbgruppe? Beweis!

2. Seien $A_1 = (S_1, \circ_1)$ und $A_2 = (S_2, \circ_2)$ Algebren, deren Trägermenge 4-elementig ist, und in denen alle Elemente rechte Einselemente sind.

   Zeigen Sie, dass A_1 und A_2 isomorph sind.

Hausaufgabe 2 (5 Punkte)

Wir betrachten Algebren $A = (S, \circ)$ mit einer 2-elementigen Trägermenge $S = \{a, b\}$ und einem 2-stelligen Operator $\circ$. Bekanntlich gibt es 16 verschiedene Algebren dieser Art, auf die wir uns im Folgenden beziehen.

1. Geben Sie eine Verknüpfungstafel für einen nicht assoziativen und gleichzeitig nicht kommutativen Operator $\circ$ an.

2. Geben Sie eine Verknüpfungstafel für einen Operator $\circ$ an, der kommutativ und gleichzeitig nicht assoziativ ist.

Hausaufgabe 3 (5 Punkte)

Wir fassen die aussagenlogischen Werte t (wahr) und f (falsch) zur booleschen Menge $\mathbb{B} = \{t, f\}$ zusammen und betrachten den aussagenlogischen Operator $\otimes : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ des „ausschließenden Oder“ (gleichbedeutend mit $\not\equiv$).

1. Zeigen Sie die Kommutativität und die Assoziativität von $\otimes$, d.h. $x \otimes y \equiv y \otimes x$ und $(x \otimes y) \otimes z \equiv x \otimes (y \otimes z)$ für alle $x, y, z \in \mathbb{B}$, durch Auswertung der entsprechenden Wahrheitswerttabellen.

2. Wir betrachten die Algebra $A = (\mathbb{B}, \otimes)$. Geben Sie einen Isomorphismus f von A auf $(\mathbb{Z}_2, +_2)$ an und beweisen Sie die entsprechende Homomorphieeigenschaft für f.

3. Stellen Sie einen wesentlichen Zusammenhang her zur Tutoraufgabe 3 von Blatt 5.

Hausaufgabe 4 (5 Punkte)

Zeigen Sie mit Hilfe von Ergebnissen aus Tutoraufgabe 4 von Blatt 5, dass jede Gruppe mit 4 Elementen kommutativ ist.

Zusatzaufgabe 3 (Repetitorium ohne Abgabe)

Wir betrachten die Teilmenge $S = \{10, 20, 30, 40, 50, 60\}$ der natürlichen Zahlen und eine binäre Relation $R \subseteq S \times S$ mit

$$R = \{(10, 20), (20, 30), (30, 50), (50, 40), (40, 20), (50, 60), (60, 60)\}\,.$$

Wir können R graphisch mit Punkten für $x \in S$ und Pfeilen für $(x, y) \in R$ darstellen und benützen auch die Schreibweise xRy für $(x, y) \in R$.

Beweisen Sie die folgenden Aussagen. Bedenken Sie dabei, dass Beweise über endliche, extensional durch Auflistung gegebene Relationen und Eigenschaften meist eine vollständige Fallunterscheidung für alle Elemente der betreffenden Mengen erfordern.

1. Für alle $x \in S$ gilt $x \bmod 2 = 0$
   $\{$i.Z. $(\forall x \in S)[x \bmod 2 = 0]\}$.
2. Für alle $x, y \in S$ gilt: falls xRy, dann gilt $y - x \leq 10$
   $\{$i.Z. $(\forall x, y \in S)[xRy \Rightarrow y - x \leq 10]\}$.
3. Es gilt nicht für alle $x \in S$ die Aussage xRx
   $\{$i.Z. $\neg(\forall x \in S)[xRx]\}$.
4. Es gilt nicht für alle $x, y \in S$: falls xRy, dann gilt $x \leq y$
   $\{$i.Z. $\neg(\forall x, y \in S)[xRy \Rightarrow x \leq y]\}$.
5. Es gibt $x, y \in S$, so dass die Aussagen xRy und $y < x$ gelten
   $\{$i.Z. $(\exists x, y \in S)[xRy \wedge y < x]\}$.
6. Es gibt ein $x \in S$, so dass für alle $y \in S$ die Aussage yRx nicht gilt
   $\{$i.Z. $(\exists x \in S\, \forall y \in S)[\neg yRx]\}$.
7. Für alle $x \in S$ gilt: falls $x \neq 10$, dann gibt es ein $y \in S$, so dass die Aussage yRx gilt $\{$i.Z. $(\forall x \in S)[x \neq 10 \Rightarrow (\exists y \in S)[yRx]]\}$.
8. Für alle $x \in S$ gibt es ein $y \in S$, so dass gilt: falls $x \neq 10$, dann gilt yRx
   $\{$i.Z. $(\forall x \in S\, \exists y \in S)[x \neq 10 \Rightarrow yRx]\}$.

Ersetzen Sie nun in den obigen Aussagen die Relation R durch ihre transitive Hülle $T = R^t$. Welche Aussagen sind nach dieser Substitution wahr geblieben?

Gibt es eine Relation $R' \subseteq S \times S$, für die gleichzeitig alle obigen Aussagen 2. bis 8. falsch sind?

Hinweis: *Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 1

In gewissen kommutativen Ringen $R = \langle S, +, \cdot, 0, 1\rangle$ stellt sich der erweiterte Euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers $\mathrm{ggT}(a, b)$ zweier Elemente $a \in S$ und $b \in S$ dar als eine iterierte Transformation (Matrixmultiplikation) Q_i angewandt auf Δ_{i-1} wie folgt mit $r_0 = a$ und $r_1 = b$.

$$\Delta_0 = \begin{pmatrix} a \\ b \end{pmatrix}, \ \Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_i \Delta_{i-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}, \ i := 1, 2, \ldots, n \in \mathbb{N}\,.$$

Dabei werden die Quotienten q_i so gewählt (geschätzt), dass die Δ_i mit wachsendem i in einem gewissen Sinn stets echt kleiner werden. Eine Berechnung wird beendet, wenn die Folge der Δ_i maximale Länge besitzt, d. h. wenn kein Quotient existiert, der die Bildung eines noch kleineren Restes erlaubt. Zur Bemessung der Größe von Elementen eines Ringes dient beispielweise im Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ die Betragsfunktion. In Polynomringen wird der Grad eines Polynoms verwendet.
Wir betrachten im Folgenden den Ring $(\mathbb{Z}, +, \cdot, 0, 1)$ der ganzen Zahlen.

1. Zeigen Sie für alle entsprechenden i

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(r_i, r_{i+1}).$$

2. Berechnen Sie mit dem Euklidischen Algorithmus den $\mathrm{ggT}(10800, 122)$.

Vorbereitung 2

Mit $R = \mathbb{Z}_3[x]$ bezeichnen wir den Ring aller Polynome über einer Variablen x mit Koeffizienten aus dem Körper $(\mathbb{Z}_3, +_3, \cdot_3)$ der ganzen Zahlen modulo 3.
Seien $a(x), b(x) \in R$ gegeben durch

$$\begin{aligned} a(x) &= x^6 + 2x^4 + 2x^3 + x^2 + 1\,, \\ b(x) &= x^3 + x^2 + 1\,. \end{aligned}$$

1. Bestimmen Sie Polynome $r_2(x), r_3(x), q_1(x), q_2(x) \in R$ mit
   $\mathrm{grad}(r_3(x)) < \mathrm{grad}(r_2(x)) < \mathrm{grad}(b(x))$, so dass die folgenden Gleichungen gelten.

$$\begin{aligned} r_2(x) &= a(x) - q_1(x) \cdot b(x)\,, \\ r_3(x) &= b(x) - q_2(x) \cdot r_2(x)\,. \end{aligned}$$

2. Bestimmen Sie ein Polynom $t(x) \in R$ möglichst hohen Grades, das ein gemeinsamer Teiler von $a(x)$ und $b(x)$ ist.

Vorbereitung 3

Bestimmen Sie Polynome $a(x),\ b(x) \in \mathbb{Q}[x]$, so dass gilt

$$\frac{x^2 + x}{(x^2 + 1)(x^2 + 2)} = \frac{a(x)}{x^2 + 1} + \frac{b(x)}{x^2 + 2}\,.$$

Tutoraufgabe 1

Berechnen Sie mit dem erweiterten Euklidischen Algorithmus ganze Zahlen m, n, so dass

$$81m + 128n = 1.$$

Tutoraufgabe 2

Wir betrachten die multiplikative Gruppe $(\mathbb{Z}^*_{1000}, \cdot_{1000}, 1)$ mit
$\mathbb{Z}^*_{1000} = \{x \in \mathbb{N}\,;\, x < 1000 \text{ und } \operatorname{ggT}(1000, x) = 1\}$.

1. Führen Sie den Euklidischen Algorithmus aus, um den größten gemeinsamen Teiler von 1000 und 69 zu berechnen. Protokollieren Sie die Berechnungsschritte.

2. Berechnen Sie auf der Grundlage Ihres Protokolls der Berechnung des $\operatorname{ggT}(1000, 69)$ Zahlen $a, b \in \mathbb{Z}$, so dass gilt

$$a \cdot 1000 + b \cdot 69 = \operatorname{ggT}(1000, 69)\,.$$

3. Es gilt $69 \in \mathbb{Z}^*_{1000}$. Bestimmen Sie in der multiplikativen Gruppe $(\mathbb{Z}^*_{1000}, \cdot_{1000}, 1)$ das Inverse $(69)^{-1}$ von 69.

Tutoraufgabe 3

Bestimmen Sie mit dem erweiterten Euklidischen Algorithmus einen größten gemeinsamen Teiler der Polynome $x^5 - 5x^4 + 4x^3 + 2x^2 - 12x + 10$ und $x^2 - 1$. Dabei werden

1. die Polynome im Ring $\mathbb{Q}[x]$ betrachtet.

2. die Polynome im Ring $\mathbb{Z}_{13}[x]$ betrachtet.

Tutoraufgabe 4

Gegeben sei der Bruch $f(x) = \frac{p(x)}{q(x)}$ mit den Polynomen $p(x), q(x) \in \mathbb{C}[x]$,

$$p(x) = 3x^3 - 52x + 16 \quad \text{und} \quad q(x) = x^4 - x^3 - 8x^2 - 4x - 48\,.$$

1. Man bestimme einen größten gemeinsamen Teiler $r(x)$ von $p(x)$ und $q(x)$ und dividiere Zähler und Nenner von $f(x)$ durch $r(x)$. Das Ergebnis nennen wir den vollständig gekürzten Bruch $F(x)$.

2. Bestimmen Sie die vollständige Partialbruchzerlegung von $F(x)$, d. h., berechnen Sie $\alpha, \beta, \gamma, A, B, C \in \mathbb{C}$ so, dass gilt

$$F(x) = \frac{A}{x+\alpha} + \frac{B}{x+\beta} + \frac{C}{x+\gamma}\,.$$